

**IN THE UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF ILLINOIS**

Jonathan Switzer	)	
Sharon Bartosiak	)	Case No. 3:13-cv-01319-DRH-PMF
Lisa Gerber,	)	
	)	
Plaintiffs,	)	JURY TRIAL DEMANDED
	)	
vs.	)	
	)	
TARGET CORPORATION, a Minnesota	)	
corporation,	)	
	)	
Defendant.	)	

**CLASS ACTION COMPLAINT**

NOW COMES the Plaintiffs, on behalf of themselves and all others similarly situated, and for their class action complaint state as follows:

**NATURE OF THE ACTION**

1. Plaintiffs bring this class action as a result of a breach of the security system of Defendant Target Corporation (“Target”) governing electronic transactions, resulting in compromised security of Plaintiffs’ and Class Members’ personal financial information. Such personal information included, but upon information and belief was not limited to, the putative Class Members’ (hereafter “Class Members”) names, credit or debit card number, the card’s expiration date, and the card’s CVV (a three-digit security code) (“Personal Information”).

2. Target has admitted publicly that between November 27, 2013, and December 15, 2013, credit and debit cards in its United State stores were compromised, with the result that Personal Information of Plaintiffs and Class Members’ Personal Information was used or is at risk of use in fraudulent transactions around the world. Target has expressly identified the danger and/or occurrence of “suspicious” and “unusual” activity threatening Plaintiffs and Class

Members, including “misuse . . . of credit and debit information,” and “incidents of fraud and identity theft.”

3. Upon information and belief, Target operates nearly 1,800 stores nationwide, and Target’s security failures affected the credit and debit card of millions of customers, including Plaintiffs and Class Members. Target has publicly stated: “Approximately 40 million credit and debit card accounts may have been impacted . . .”

4. Target further confessed that, if Plaintiffs and Class Members seek to protect themselves from further damages resulting from Target’s security failures by adding a fraud alert to Plaintiffs’ and Class Members’ credit report files, it “may delay your ability to obtain credit.”

5. Upon information and belief, the security breach and theft of Personal Information was caused by Target’s violations of its obligations to abide by the best practices and industry standards concerning the security of its payment processing systems and the computers associated therewith as set forth, for example, in Payment Card Industry Security Standards Council Data Security Standards (“PCI DSS”) and the decisions of the Federal Trade Commission (“FTC”) concerning protection of consumer financial information.

6. After learning of the security breach, Target failed to notify Plaintiffs and the putative Classes in a timely manner and failed to take other reasonable steps to inform them of the nature and extent of the breach. As a result, Target prevented Plaintiffs and the putative Class Members from protecting themselves from the breach and caused Plaintiffs and Class Members to suffer financial loss.

7. Plaintiffs, on behalf of themselves and all others similarly situated, assert the following claims: Violations of the Stored Communications Act (“SCA”), 18 U.S.C. § 2702; negligence; breach of implied contract; violations of the Missouri Merchandising Practices Act

(“MMPA”), Mo. Rev. Stat. § 407.020, and the substantially similar statutes of the other states in which Target conducts business; and violations of the Illinois Personal Information Protection Act (“IPIPA”), 815 ILCS 530/1, and the substantially similar statutes of the other states in which Target conducts business.

**JURISDICTION AND VENUE**

8. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331, which confers upon the Court original jurisdiction over all civil actions arising under the laws of the United States, and pursuant to 18 U.S.C. § 2707. This Court has supplemental jurisdiction over Plaintiffs’ and Class Members’ state law claims under 28 U.S.C. § 1337.

9. In addition, this Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all Members of the putative Classes are in excess of \$5,000,000.00, exclusive of interest and costs, and many of the Members of the putative Classes are citizens of different states than Defendant. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d).

10. Venue is properly set in this District pursuant to 28 U.S.C. § 1331(b) since Target transacts business and is found within this judicial district. Likewise, a substantial part of the events giving rise to the claim occurred within this judicial district.

**PARTIES**

11. Plaintiff Jonathan Switzer is domiciled in Millstadt, Illinois and is a citizen of Illinois. On or about December 9, 2013, Switzer shopped at Target in Belleville, Illinois and swiped his debit card through a Target pin pad terminal. On information and belief Switzer’s Personal Information was compromised as a result of Target’s security failures. As a result of

such compromise, Switzer suffered losses and damages in an amount yet to be completely determinable as such losses and damages are ongoing.

12. Plaintiff Sharon Bartosiak is domiciled in Mascoutah, Illinois and is a citizen of Illinois. On or about December 2, 2013, Bartosiak shopped at Target in Shiloh, Illinois and swiped her debit card through a Target pin pad terminal. On information and belief Bartosiak's Personal Information was compromised as a result of Target's security failures. As a result of such compromise, Bartosiak suffered losses and damages in an amount yet to be completely determined as such losses and damages are ongoing.

13. Plaintiff Lisa Gerber is domiciled in Florissant, Missouri and is a citizen of Missouri. On or about December 14, 2013, Gerber shopped at Target locations in Cave Springs, Missouri, Bridgeton, Missouri and/or Florissant, Missouri, and swiped her debit card through Target's pin pad terminal(s). On information and belief Gerber's Personal Information was compromised as a result of Target's security failures. As a result of such compromise, Gerber suffered losses and damages in an amount yet to be determined, including but not limited to approximately \$600-700 withdrawn from her bank account without authorization, loss of use of her bank accounts during a period of time while such cards were frozen, loss of use of her bank accounts while she did not have an active and/or usable debit/credit card, and other losses and damages in an amount yet to be completely determined as such losses and damages are ongoing.

14. Target is a corporation organized under Minnesota law with its headquarters and principal place of business in Minneapolis, Minnesota.

#### **FACTUAL BACKGROUND**

15. Target accepts customer payments for purchase through credit and debit cards issued by members of the payment card industry ("PCI") such as Visa or MasterCard.

16. In 2006, the PCI members established a Security Standards Counsel (“PCI SSC”) as a forum to develop PCI Data Security Standards (“PCI DSS”) for increased security of payment processing systems.

17. The PCI DSS provides, “If you are a merchant that accepts payment cards, you are required to be compliant with the PCI Data Security Standard.” Target is a merchant that accepts payment cards.

18. The PCI DSS requires a merchant to:

a. **Assess**—identify cardholder data, take inventory of IT assets and business processes for payment card processing, and analyze them for vulnerabilities that could expose cardholder data.

b. **Remediate**—fix vulnerabilities and do not store cardholder data unless needed.

c. **Report**—compile and submit required remediation validation records (if applicable) and submit compliance reports to the acquiring bank and card brands with which a merchant does business.

19. Additionally, since 1995, the FTC has been studying the manner in which online entities collect and use personal information and safeguards to assure that online data collection practice is fair and provides adequate information privacy protection. The result of this study is the FTC Fair Information Practice Principles. The core principles are:

a. **Notice/Awareness**--Consumers should be given notice of an entity’s information practices before any personal information is collected from them. This requires that companies explicitly notify of some or all of the following:

- Identification of the entity collecting the data;

- Identification of the uses to which the data will be put;
- Identification of any potential recipients of the data;
- The nature of the data collected and the means by which it is collected;
- Whether the provision of the requested data is voluntary or required; and
- The steps taken by the data collector to ensure the confidentiality, integrity and quality of the data.

b. **Choice/Consent**--Choice and consent in an online information-gathering

sense means giving consumers options to control how their data is used with respect to secondary uses of information beyond the immediate needs of the information collector to complete the consumer's transaction.

c. **Access/Participation**--Access as defined in the Fair Information Practice

Principles includes not only a consumer's ability to view the data collected, but also to verify and contest its accuracy. This access must be inexpensive and timely in order to be useful to the consumer.

d. **Integrity/Security**--Information collectors should ensure that the data

they collect is accurate and secure. They should improve the integrity of data by cross-referencing it with only reputable databases and by providing access for the consumer to verify it. Information collectors should keep their data secure by protecting against both internal and external security threats. They should limit access within their company to only necessary employees to protect against internal threats, and they should use encryption and other computer-based security systems to stop outside threats.

e. **Enforcement/Redress**--In order to ensure that companies follow the Fair

Information Practice Principles, there must be enforcement measures. The FTC identifies three

types of enforcement measures: self-regulation by the information collectors or an appointed regulatory body; private remedies that give civil causes of action for individuals whose information has been misused to sue violators; and government enforcement, which can include civil and criminal penalties levied by the government.

20. On information and belief, Target failed adequately to analyze its computer systems for vulnerabilities that could expose cardholder data. Target further failed to fix the vulnerabilities in its computer systems which allowed Plaintiffs' and Class Members' Personal Information to become compromised.

21. Additionally, on information and belief, Target unlawfully collected consumer financial data for marketing purposes beyond the needs of specific transactions, in order to accrue financial benefit at the risk and likelihood of compromising consumers' Personal Information.

22. As a result, Target allowed Personal Information connected with 40,000,000 consumers' credit cards and debit cards, including credit cards and debit cards of Plaintiffs and Class Members, to become compromised for a minimum period between November 27, 2013 and December 15, 2013.

23. Target became aware of its security failures and the theft of its customer Personal Information, including the Personal Information of Plaintiffs and Class Members, no later than December 18, 2013.

24. To date, Target has not provided individual notification to Plaintiffs and Class Members of Target's security failures.

25. Also, to date, Target has not reimbursed Plaintiffs and Class Members for financial losses caused by Target's security failures.

26. Plaintiffs and Class Members are subject to continuing damage from having their Personal Information comprised as a result of Target's inadequate systems and failures. Such damages include, among other things, out-of-pocket expenses incurred to mitigate the increased risk of identity theft and or fraud; credit, debit, and financial monitoring to prevent and/or mitigate theft, identity theft, and/or fraud incurred or likely to occur as a result of Target's security failures; the value of their time and resources spent mitigating the identity theft and/or fraud; the cost of and time spent replacing credit cards and debit cards and reconfiguring automatic payment programs with other merchants related to the compromised cards; and irrecoverable financial losses due to unauthorized charges on the credit/debit cards of Target customers by identity thieves who wrongfully gained access to the Personal Information of Plaintiffs and the Classes.

#### **CLASS ACTION ALLEGATIONS**

27. Plaintiffs bring this action on their own behalf and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following three (3) multi-state classes:

All persons who shopped at Defendant's locations, whose Personal Information was subject to Target's security failures and who suffered damages in the loss of time and use of their credit and debit cards until such time as replacement cards could be obtained.

All persons who shopped at Defendant's locations, whose Personal Information was subject to Target's security failures and who suffered damages in the amount of fraudulent charges / unauthorized withdrawals made to their credit and/or debit cards or suffered damages in the amount of overdraft charges made to their credit and/or debit cards.

All persons who shopped at Defendant's locations, whose Personal Information was subject to Target's security failures and who have suffered or anticipate suffering damages, loss, and/or expenses accruing due to Target's security failures.

Excluded from the Classes are Target and its affiliates, parents, subsidiaries, employees, officers, agents, and directors.

28. The Members of the Classes are so numerous that joinder of all Members is impracticable. Target has publicly admitted that up to 40 million credit and/or debit cards may have been compromised, and the Members of the Classes are geographically dispersed. Disposition of the claims of the proposed Classes in a class action will provide substantial benefits to both the parties and the Court.

29. The rights of each member of the proposed Classes were violated in a similar fashion based upon Target's uniform wrongful actions and/or inaction.

30. The following questions of law and fact are common to each proposed Class Member and predominate over questions that may affect individual Class Members:

- a. Whether Target failed to use reasonable care and commercially reasonable methods to secure and safeguard its customers' private financial information;
- b. Whether Target properly implemented its purported security measures to protect consumers' private financial information from unauthorized capture, dissemination and misuse;
- c. Whether Target took reasonable measures to determine the extent of the security breach after it first learned of the same;
- d. Whether Target's delay in informing consumers of the security breach was unreasonable;
- e. Whether Target's method of informing consumers of the security breach and its description of the breach and potential exposure to damages as a result of the same was unreasonable;
- f. Whether Target's conduct violated the Stored Communications Act, 18 U.S.C. § 2702;

- g. Whether Target breached an implied contract with Class Members;
- h. Whether Target's conduct violated the Missouri Merchandising Practices Act, Mo. Rev. Stat. § 407.020, and the substantively similar statutes of the other states where Target conducts business;
- i. Whether Target's conduct violated the Illinois Personal Information Protection Act, 815 ILCS 530/1, and the substantially similar statutes of the other states in which Target conducts business; and
- j. Whether Plaintiffs and others Members of the Classes are entitled to compensation, monetary damages, equitable relief and injunctive relief, and, if so, the nature and amount of such relief.

31. Plaintiffs' claims are typical of the claim of absent Class Members. If brought individually, the claim of each Class Member would necessarily require proof of the same material and substantive facts, and seek the same remedies.

32. The Plaintiffs are willing and prepared to serve the Court and the proposed Classes in a representative capacity. The Plaintiffs will fairly and adequately protect the interest of the Classes and have no interests adverse to, or which directly and irrevocably conflicts with, the interests of other Members of the Classes. Further, Plaintiffs have retained counsel experienced in prosecuting complex class action litigation.

33. Target has acted or refused to act on grounds generally applicable to the proposed Classes, thereby making appropriate equitable relief with respect to the Classes.

34. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual claims by the Class Members are impractical, as the costs of prosecution may exceed what any Class Member has at stake.

35. Members of the Classes are readily ascertainable through Target's records of the purchases made at its stores.

36. Prosecuting separate actions by individual Class Members would create a risk of inconsistent or varying adjudications that would establish incomparable standards of conduct for Target. Moreover, adjudications with respect to individual Class Members would, as a practical matter, be dispositive of the interests of other Class Members.

### **CAUSES OF ACTION**

#### **COUNT I – VIOLATION OF THE FEDERAL STORED COMMUNICATIONS ACT, 18 U.S.C. § 2702**

37. Plaintiffs repeat, reallege, and incorporate paragraphs 1-40 in this Complaint as if fully set forth herein.

38. The Stored Communications Act (“SCA”) contains provisions that provide consumers with redress if a company mishandles their electronically stored information. The SCA was designed, in relevant part, “to protect individuals’ privacy interests in personal and proprietary information.” S. Rep. No. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555 at 3557.

39. Section 2702(a)(1) of the SCA provides that “a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service.” 18 U.S.C. § 2702(a)(1).

40. The SCA defines “electronic communication service” as “any service which provides to users thereof the ability to send or receive wire or electronic communications.” *Id.* at § 2510(15).

41. Through its payment processing equipment, Target provides an “electronic communication service to the public” within the meaning of the SCA because it provides consumers at large with credit and debit card payment processing capability that enables them to send or receive wire or electronic communications concerning their private financial information to transaction managers, card companies, or banks.

42. By failing to take commercially reasonable steps to safeguard sensitive private financial information, even after Target was aware that customers’ Personal Information had been compromised, Target has knowingly divulged customers’ private financial information that was communicated to financial institutions solely for customers’ payment verification purposes, while in electronic storage in Target’s payment system.

43. Section 2702(a)(2)(A) of the SCA provides that “a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service.” 18 U.S.C. § 2702(a)(2)(A).

44. The SCA defines “remote computing service” as “the provision to the public of computer storage or processing services by means of an electronic communication system.” 18 U.S.C. § 2711(2).

45. An “electronic communications systems” is defined by the SCA as “any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.” 18 U.S.C. § 2510(4).

46. Target provides remote computing services to the public by virtue of its computer processing services for consumer credit and debit card payments, which are used by customers and carried out by means of an electronic communications system, namely the use of wire, electromagnetic, photooptical or photoelectric facilities for the transmission of wire or electronic communications received from, and on behalf of, the customer concerning customer private financial information.

47. By failing to take commercially reasonable steps to safeguard sensitive private financial information, Target has knowingly divulged customers' private financial information that was carried and maintained on Target's remote computing service solely for the customer's payment verification purposes.

48. As a result of Target's conduct described herein and its violations of Section 2702(a)(1) and (2)(A), Plaintiffs and putative Class Members have suffered injuries, including lost money and the costs associated with the need for vigilant credit monitoring to protect against additional identity theft. Plaintiffs, on their own behalf and on behalf of the putative Classes, seek an order awarding themselves and the Classes the maximum statutory damages available under 18 U.S.C. § 2707 in addition to the cost for 3 years of credit monitoring services.

## **COUNT II – NEGLIGENCE**

49. Plaintiffs repeat, reallege, and incorporate the preceding paragraphs of this Complaint as if fully set forth herein.

50. Upon coming into possession of Plaintiffs' and Class Members' Personal Information, i.e., private, non-public, sensitive financial information, Target had (and continues to have) a duty to exercise reasonable care in safeguarding and protecting the information from being compromised and/or stolen.

51. Target also had a duty to timely disclose to Plaintiffs and Class Members that a breach of security had occurred and their Personal Information pertaining to their credit cards and/or debit cards had been compromised, or was reasonably believed to be compromised.

52. Target also had a duty to put into place internal policies and procedures designed to detect and prevent the theft or dissemination of Plaintiffs' and Class Members' Personal Information.

53. Target, by and through its above negligent acts and/or omissions, breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding their Personal Information which was in Target's possession, custody, and control.

54. Target, by and through its above negligent acts and or omissions, further breached its duty to Plaintiffs and Class Members by failing to put into place internal policies and procedures designed to detect and prevent the unauthorized dissemination of Plaintiffs and Class Members' Personal Information.

55. Target, by and through its above negligent acts and or omissions, breached its duty to timely disclose the fact that Plaintiffs' and Class Members' Personal Information had been or was reasonable believed to be have been compromised.

56. Target's negligent and wrongful breach of its duties owed to Plaintiffs and Class Members, their Personal Information would not have been compromised.

57. Plaintiffs' and Class Members' Personal Information was compromised and/or stolen as a direct and proximate result of Target's breach of its duties as set forth herein.

58. Plaintiffs and Class Members have suffered actual damages including, but not limited to, having their personal information compromised, incurring time and expenses in cancelling their debit and/credit cards, activating new cards and re-establishing automatic

payment authorizations from their new cards, and other economic and non-economic damages, including irrecoverable losses due to unauthorized charges on their credit/debit cards.

**COUNT III -- BREACH OF IMPLIED CONTRACT**

59. Plaintiffs repeat, reallege, and incorporate the foregoing paragraphs of this Complaint as if fully set forth herein.

60. Plaintiffs and Class Members were required to provide Target with their Personal Information in order to facilitate their credit card and/or debit card transactions.

61. Implicit in this requirement was a covenant requiring Target to take reasonable efforts to safeguard this information and promptly notify Plaintiffs and Class Members in the event their information was compromised.

62. Similarly, it was implicit that Target would not disclose Plaintiffs' and Class Members' Personal Information.

63. Notwithstanding its obligations, Target knowingly failed to safeguard and protect Plaintiffs' and Class Members' Personal Information. To the contrary, Target allowed this information to be disseminated to unauthorized third parties.

64. Target's above wrongful actions and/or inaction breached its implied contracts with Plaintiffs and Class Members, which in turn directly and/or proximately caused Plaintiffs and Class Members to suffer substantial injuries.

**COUNT IV – VIOLATION OF THE MISSOURI MERCHANDISING  
PRACTICES ACT AND SUBSTANTIALLY SIMILAR STATUTES OF  
THE OTHER STATES WHERE DEFENDANT DOES BUSINESS**

65. Plaintiffs repeat, reallege, and incorporate the foregoing paragraphs of this Complaint as if fully set forth herein.

66. Target violated the Missouri Merchandising Practices Act, Mo. Rev. Stat. § 407.020, and the substantially similar statutes of the other states in which it conducts business by failing to properly implement adequate, commercially reasonable security measures to protect customers' private financial information, and by failing to immediately notify affected customers of the nature and extent of the security breach.

67. Target's fraudulent and deceptive omissions and misrepresentations regarding the company's security measures to protect customers' private financial information and the extent of the breach of those security measures were intended to deceive and induce Plaintiffs and the putative Class Members' reliance on Target's misrepresentations that their financial information was secure and protected when using debit and credit cards to shop at Target stores.

68. Target's unlawful misrepresentations and omissions occurred in the course of conduct involving trade or commerce.

69. Target's unlawful misrepresentations and omissions were material because Plaintiffs and the other putative Class Members, if they had known the truth, would not have risked compromising their private financial information by using their debit or credit cards at Target stores. Plaintiffs and the other putative Class Members would consider the omitted and misrepresented material facts important in making their purchasing decisions.

70. Target's unlawful misrepresentations and omissions damaged Plaintiffs and the other putative Class Members because Plaintiffs and Class Members would not have chosen to

expose their private financial information to a security breach and subsequent exploitation by the defrauders.

71. Plaintiffs, individually and on behalf of the putative Classes, seek an order requiring Defendant to pay: monetary and punitive damages for the conduct described herein; three years of credit card fraud monitoring services for Plaintiffs and Members of the putative Classes; and the reasonable attorney's fees and costs of suit of Plaintiffs and Class Members; together with all such other and further relief as may be just.

**COUNT V -- VIOLATION OF THE ILLINOIS PERSONAL INFORMATION PROTECTION ACT AND SUBSTANTIALLY SIMILAR STATUTES OF THE OTHER STATES WHERE DEFENDANT DOES BUSINESS**

72. Plaintiffs repeat, reallege, and incorporate the foregoing paragraphs of this Complaint as if fully set forth herein.

73. At all times relevant hereto, there was in full force and effect the Illinois Personal Information Protection Act (IPIPA), 815 ILCS 530/1, together with other relevant state statutes providing that any data collector that owns or licenses personal information concerning a state resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach.

74. The relevant statutes provide that disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

75. Target is a data collector within the meaning of the IPIPA and other relevant statutes.

76. Target came into possession of Plaintiffs' and Class Members' personal information, as that is defined by the IPIPA and other relevant statutes.

77. Target had a duty to disclose in the most expedient time possible and without unreasonable delay the breach of the security of the system data.

78. Target, through its actions and/or omissions, failed to disclose in the most expedient time possible and without unreasonable delay the breach of the security of the system data.

79. Target's failure to timely disclose is a violation of the IPIPA and other relevant statutes.

80. Plaintiffs and Class Members request that an injunction be issued to require Target to comply with the IPIPA and other relevant statutes.

81. To the extent that a violation of the IPIPA and other relevant statutes also constitutes a violation of pertinent state consumer protection laws, *see, e.g.*, Section 20 of the IPIPA, providing that a violation of this IPIPA constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, Target's violation of the IPIPA and other pertinent statutes is also a violation of pertinent state consumer protection law.

**JURY TRIAL DEMAND**

Plaintiffs and class members demand a jury trial as to all claims and issues triable of right by a jury.

**PRAAYER FOR RELIEF**

WHEREFORE, Plaintiffs and the Members of the proposed Classes pray that this Honorable Court do the following:

- A. Certify the matter as a class action pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure and order that notice be provided to all Class Members;
- B. Designate Plaintiffs as representative of the Classes and the undersigned counsel as Class Counsel;
- C. Award Plaintiffs and the Classes compensatory and punitive damages in an amount to be determined by the trier of fact;
- D. Award Plaintiffs and the Classes statutory interest and penalties;

- E. Award Plaintiffs and the Classes appropriate injunctive and/or declaratory relief;
- F. Award Plaintiffs and the Classes their costs, prejudgment interest, and attorney fees; and
- G. Grant such other relief as is just and proper.

Respectfully submitted,  
THE DRISCOLL FIRM, P.C.

By: /s/John J. Driscoll  
John J. Driscoll, #6276464  
211 N. Broadway, 40<sup>th</sup> Floor  
St. Louis, Missouri 63102  
314-932-3232 telephone  
314-932-3233 facsimile